The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/29/2020

SUBJECT:
Multiple Vulnerabilities in ArubaNetworks ArubaOS and SD-WAN Could Allow for Arbitrary Code Execution.

OVERVIEW:
Multiple vulnerabilities have been discovered in ArubaNetwork's ArubaOS and SD-WAN, which could result in arbitrary code execution. Aruba (a Hewlett Packard Enterprise company) is the worldwide second-largest enterprise WLAN vendor after Cisco. ArubaOS is its WLAN controller system for automating WLAN management, and SD-WAN (software defined WAN) is its cloud-oriented WAN orchestration system. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in context of the user running the application.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild. The vulnerabilities were discovered by a researcher via Aruba's bug bounty program.

SYSTEMS AFFECTED:
Buffer Overflow (CVE-2020-24633):
- ArubaOS 6.4.4.23, 6.5.4.17, 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below
- SD-WAN 2.1.0.1, 2.2.0.0 and below

Unauthenticated Remote Command Injection (CVE-2020-24634):
- ArubaOS 8.2.2.9, 8.3.0.13, 8.5.0.10, 8.6.0.5, 8.7.0.0 and below
- SD-WAN 2.1.0.1, 2.2.0.0 and below

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in ArubaNetwork's ArubaOS and SD-WAN, which could result in arbitrary code execution. The vulnerabilities are as follows:

- Buffer overflow caused by specially crafted packets sent to the PAPI (Process API, Aruba's access point management protocol) on UDP port 8211 of access points or controllers. [CVE-2020-24633]
- Unauthenticated remote command injection caused by specially crafted packets sent to the PAPI (Process API, Aruba's access point management protocol) on UDP port 8211 of access points or controllers. [CVE-2020-24634]

An attacker can exploit these vulnerabilities to run arbitrary commands in the context of the user running the application. Due to the central location of the attack targets, an attacker could use a successful exploit as a foothold to pivot through the network and/or set up interception attacks (e.g. Man in the Middle) with their control over the WLAN/WAN.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the patches released by Aruba and upgrade software where applicable.
- Restrict communications between Controllers/Gateways via VLANs and/or firewall policies.
- Block external access at the network boundary and if possible, restrict server access to trusted hosts only.
- Apply the Principle of Least Privilege to all systems and services; run all software as a nonprivileged user with minimal access rights.
- Deploy NIDS to monitor network traffic for signs of anomalous or suspicious activity. This includes but is not limited to requests that include NOP sleds and unexplained incoming and outgoing traffic. This may indicate exploit attempts or activity that results from successful exploits.

REFERENCES:
Aruba:
https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-012.txt

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24633
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24634